International Journal of Communication 11(2017), 1–20 1932–8036/20170005

Enabling Digital Citizenship? The Reshaping of Surveillance Policy After Snowden

ARNE HINTZ
Cardiff University, UK

IAN BROWN
Oxford University, UK

The revelations by NSA whistleblower Edward Snowden have led to policy reform debates in several countries and to policy change in some, including a new legislative framework in the UK—the Investigatory Powers Act. In this article, we trace the forces and dynamics that have shaped this particular policy response. We investigate key controversies over the types and extent of surveillance; the capacity of different stakeholders to intervene into the debate and shape its outcomes; the attempts to achieve democratic legitimacy for data collection; and the consequences for digital citizenship. Drawing from a systematic analysis of relevant policy documents and interviews with key policy experts and stakeholders, we analyze conflicts over both the direction and details of surveillance policy, and uncover unequal degrees of influence over policy reform for different stakeholders. As a result, policy reform has led to a confirmation, rather than restriction, of data collection. Digital citizenship may be supported by the (limited) policy review in the UK and the development of a more transparent legislative framework, but is impeded by a growing range of surveillance capabilities.

Keywords: Snowden, surveillance, policy, law, regulation, digital citizenship, Investigatory Powers Bill, Investigatory Powers Act

Engagement with our social, political, and cultural environments is increasingly mediated through digital platforms. Citizens interact with public services through online tools, participate in online campaigns, express themselves online, share information and culture, and thus develop agency through digital environments. The evolution of these practices depends on a variety of factors, including the stability and integrity of the technical infrastructure, its accessibility, changes in cultural practices, and the legal and regulatory environment. Policies created by governments and Internet businesses are crucial in either enabling or restricting the various activities of online citizens. Policy debates on how state and commercial actors should support, limit, protect, or monitor people's digital interactions are therefore crucial moments in the shaping of digital citizenship.

Arne Hintz: HintzA@cardiff.ac.uk
Ian Brown: ian.brown@oii.ox.ac.uk
Date submitted: 2016–02–29

The revelations by whistleblower Edward Snowden of the surveillance practices of American and British intelligence agencies have been such an extraordinary moment. From early June 2013, his leaks have been published in newspapers such as *The Guardian* and newer media platforms such as *The Intercept*, exposing a range of different means by which U.S. and partner state agencies collect and analyze Internet communications. The public have learnt previously undisclosed details of how data are harvested from the Internet's backbone cables and collected from Internet companies and social media platforms. The revelations exposed efforts by the U.S. National Security Agency (NSA) and the British Government Communications Headquarters (GCHQ) to break encryption protocols and to hack into communications infrastructure. Besides high-profile cases of both business and political espionage, citizens learnt about the "bulk" collection of online data, including Web browsing histories, geolocations, text messages, and other everyday online practices.[1]

The revelations have generated heated debates regarding the extent of state interference in civic life and the protection of civil rights in the context of security. They have led to calls for policy reform, legal challenges, and court proceedings; the establishment of parliamentary review committees and independent commissions; and new policies in several countries.

In this article, we will explore these developments with a focus on one of the countries most affected by the Snowden leaks—the United Kingdom. Writing at the time of intense debate on a new law that regulates a wide range of data collection and surveillance capabilities, we analyze the breadth of different interests, controversial surveillance powers, and the role of different social forces in the shaping of a new policy environment in the UK. This allows us to understand the processes and directions of policy change at this historical juncture, when key coordinates for future digital citizenship are being designed.

This article is based on two research methods: a systematic analysis of relevant policy documents, stakeholder statements, and court decisions, and a set of semistructured interviews with policy experts and stakeholders. The interviewees encompass Parliamentarians, security and law enforcement experts, and representatives of industry, civil society, and an oversight body. They include high-profile participants in the policy debate and policy development process in the UK that were able to provide in-depth insights into the challenges of shaping the regulatory cornerstones of digital citizenship.

We will first outline the conceptual background that we adopt for this article and explain the research methods. Second, we will provide an overview of both the regulatory environment in the UK and recent post-Snowden transformations. Based on the interview findings, we will, third, discuss key controversies in the current policy reform debate and analyze the agendas and interventions of different

[1] For an overview of surveillance capabilities, see Fidler (2015) and "NSA Files" by *The Guardian* (https://www.theguardian.com/us-news/the-nsa-files). For a systematic explanation of key programs, check the database developed by the "Digital Citizenship and Surveillance Society" project (https://www.dcssproject.net/category/technology/surveillance-programmes). For a collection of all documents leaked by Snowden, see the Snowden Surveillance Archive by Canadian Journalists for Free Expression (https://snowdenarchive.cjfe.org/greenstone/cgi-bin/library.cgi).

social, political, and economic forces as well as the level of public debate. Finally, we will identify implications for the future of digital citizenship and the relations between citizens and the state.

Actors, Factors, and Contexts of Policy Reform

Media and communication policy encompasses the regulatory rules and norms that shape communication infrastructures and uses. It explores how these norms are created, based on which values and interests, and how they shift. Policy analysis thus addresses existing legislation, court rulings, and government decisions, but it is also interested in the process of policy making as political negotiation between a variety of actors and interests. It highlights the conditions and implications of interactions between social forces and examines prevalent societal norms and ideologies that underlie and advance specific policy trends (Freedman, 2008).

This multidimensional perspective is necessary as media and communications policy has become "a complex ecology of interdependent structures" with "a vast array of formal and informal mechanisms working across a multiplicity of sites" (Raboy, 2002, pp. 6–7). Classic forms of national (governmental and parliamentary) policy have "become embedded within more expansive sets of interregional relations and networks of power" (Held & McGrew, 2003, p. 3), and policy authority is located at "different and sometimes overlapping levels—from the local to the supra-national and global" (Raboy & Padovani, 2010, p. 16). Regional associations such as the European Union (EU), international institutions such as the various United Nations (UN) agencies, and world summits and trade agreements all provide regulatory frameworks (and, in the case of the EU, also judicial institutions) that affect the development of national surveillance policy.

Civil society organizations and the business sector engage with this complex environment. As institutional participants, they are increasingly part of multistakeholder processes that expand policy authority beyond governments. Internet governance has been a pioneer field for experiments in collaborative and nonstate policy making as both its history and its current institutions, such as the Internet Corporation for Assigned Names and Numbers (ICANN), demonstrate (Mueller, 2010). Further, nongovernmental organizations and businesses have staged normative interventions into policy debate by setting agendas, exerting public pressure, lobbying and public campaigns, and by lending or withdrawing legitimacy to policy goals, decisions and processes (Keck & Sikkink, 1998).

Such interventions may support policy change in the event of a "policy window" (i.e., a favorable institutional, political, and sometimes ideological setting that provides a temporary opening for affecting policy change; Kingdon, 1984). Unforeseen revelations, catastrophes, economic crises, and political change can lead to such windows of opportunity. A crisis in the social, economic, or ideological system may also cause disunity among political elites and create a dynamic in which established social orders become receptive to change. "Policy monopolies"—stable configurations of policy actors—may be weakened or broken up as political constellations change and the balance of power shifts (Meyer, 2005).

Through the development of standards and protocols that have become de facto cornerstones of communication technology, as well as "privacy by design" strategies that incorporate concerns about civil rights into the technical infrastructure, nonstate actors have also preempted other forms of regulation and

thus practiced a latent and largely invisible form of policymaking (DeNardis, 2009; Gürses, Troncoso, & Diaz, 2011; Lessig, 1999). More openly, social media platforms and other online businesses have applied "terms of service" to regulate the use of their platforms and set the conditions for free speech and privacy (Youmans & York, 2012). Complementing state policy, these forms of privatized policy making (Hintz, 2015) demonstrate a "shift of responsibility . . . onto strategically positioned private sector intermediaries" (Mueller, 2010, p. 149). This interplay of different forces in the shaping of the regulatory environment has been reflected in theoretical approaches informed by, among others, political-economic concerns (Chakravartty & Zhao, 2008; Freedman, 2008), science and technology studies (Musiani, 2015), and social movement studies (Keck & Sikkink, 1998).

The interaction of public and private actors at different levels is, furthermore, ingrained in contemporary forms of surveillance. The Snowden revelations focused largely on state surveillance by agencies such as the NSA and GCHQ, but they also pointed to state reliance on commercial telecommunications and social media platforms in gathering vast amounts of user data (Lyon, 2014). Telecommunications companies such as AT&T and British Telecom have long been active partners in state surveillance of their customers (European Parliament, 2001). Online platforms such as Facebook and Google have become key "data mines" (Andrejevic, 2012, p. 71) due to their inherent goal of maximizing (corporate) surveillance to enable targeted advertising, and the data volunteered by users to social media is analyzed by both commercial data brokers and state agencies (Trottier, 2015).

Networked data flows are thus subject to multiple processes of "veillance" (Bakir, 2015; Haggerty & Ericson, 2000). These constrain and regulate the interactions of digital citizens with their online environment (Isin & Ruppert, 2015), for example, through the "chilling effect" that may lead to caution and self-censorship when one is under observation (Hampton et al., 2014; PEN, 2013; see also the article by Dencik and Cable in this Special Section).

Methodology

This article is based on a combination of two sets of research methods to gain an in-depth understanding of surveillance policy development and its challenges and controversies. First, we conducted a systematic review of relevant policy documents, stakeholder statements, and court decisions that provide key markers of surveillance policy development in the UK. This review led to a publicly available database of policy institutions, decisions, and surveillance power.[2] The overview of UK surveillance policy in the next section is based on this work. Second, we conducted 13 semistructured interviews with policy stakeholders and experts from a variety of stakeholder communities. The interview participants are shown in Table 1.

Table 1. Interviewees.

[2] See http://www.dcssproject.net/policy/. The database was largely developed by Dr. Josh Cowls at Oxford University.

Sector	Interviewee	Marked as
Politics (Pol)	Former Member of Parliament (2010–2015) and of the Home Affairs Select Committee	Interviewee 1, Pol
	Peer in the House of Lords	Interviewee 2, Pol
	Peer in the House of Lords	Interviewee 3, Pol
Security and law enforcement (Sec)	Cybersecurity researcher and former member of the British military	Interviewee 4, Sec
	Retired senior intelligence official	Interviewee 5, Sec
	Senior law enforcement officer	Interviewee 6, Sec
Industry (Ind)	Program Manager at British technology industry trade association	Interviewee 7, Ind
	Vice president of security services company	Interviewee 8, Ind
	Policy manager at international Internet services corporation	Interviewee 9, Ind
Civil society (CS)	Director of British digital rights coalition	Interviewee 10, CS
	Policy officer of civil liberties organization	Interviewee 11, CS
	Chief executive of privacy campaign organization	Interviewee 12, CS
Review and oversight (Rev)	Official of the Interception of Communications Commissioner's Office	Interviewee 13, Rev

The interviews were carried out between August 2015 and February 2016, and thus during a time of intense debate in the UK over the introduction of a major surveillance law, the Investigatory Powers Bill. A first draft of the Bill was published in October 2015, a slightly revised version was introduced to Parliament in March 2016, and the Bill was finally adopted (and thus became the Investigatory Powers Act) in November 2016. Six of the interviews were conducted in person, seven over the phone or on Skype, lasting on average one hour. They focused on the concept of surveillance, key policy controversies, the new Bill, and the roles and interests of different stakeholders in the policy debate. The research benefitted from the fact that we had access to senior experts and key participants of the national policy debate, who not only explained core positions of their respective sector but also offered personal accounts of the policy development process. The interviews thus provided us with significant insights into the shaping of surveillance policy. The research was conducted as part of the project "Digital Citizenship and Surveillance Society: UK State-Media-Citizen Relations After the Snowden Leaks" (2014–2016).[3]

Surveillance Policy in the UK

[3] The project was funded by the UK Economic and Social Research Council.

Until 2016, law enforcement and intelligence agency data collection and analysis in the UK were regulated by a jigsaw puzzle of different laws that each address specific aspects and practices. In the following, we outline central components of this (largely) pre-Snowden regulatory framework, based on document analysis and the above-mentioned database. This policy environment has included, for example, the Data Protection Act of 1998, which controls access to and use of personal data. It provides limitations for data collection and sharing but also includes exemptions for the protection of "national security" and the prevention or detection of crime. The Regulation of Investigatory Powers Act (RIPA) from 2000, as amended by the Data Retention and Investigatory Powers Act 2014, allows a Secretary of State to authorize the interception of the communications of a specific individual but also of wide-ranging and vaguely defined types of traffic in bulk (Brown, 2014).

These more specific regulations of data interception are underpinned by older laws, such as the Telecommunications Act of 1984, which offers the Secretary of State interception powers in communications networks, and the Intelligence Services Act of 1994, which provides the core legal basis for the surveillance activities by GCHQ. While it limits GCHQ's lawful activities to "interests of national security," such interests have traditionally been broadly interpreted in UK law. More recent legislation, such as the Wireless Telegraphy Act of 2006, has updated and extended older powers for the interception of communication.

A number of oversight bodies review these surveillance capabilities and their implementation. They include, on a one-off basis, the Prime Minister's Special Envoy on Intelligence and Law Enforcement Data Sharing and the Independent Reviewer of Terrorism Legislation (appointed by the Secretary of State), and on an ongoing basis, the Intelligence Services Commissioner; the Interception of Communications Commissioner; and the Intelligence and Security Committee (ISC) of Parliament. The Investigatory Powers Tribunal (IPT) has exclusive jurisdiction to hear complaints about the intelligence agencies or interception.

These national rules, institutions, and processes are embedded in regional and international policy, such as the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), which was incorporated into UK law in the Human Rights Act of 1998. Article 8 of the Convention guarantees everyone's "right to respect for his private and family life, his home and his correspondence" (Council of Europe, 1950, Art. 8). Regional courts, such as the European Court of Human Rights (ECHR), can hear complaints about surveillance and advise on its lawfulness. Directives adopted by the European Commission—such as the Data Retention Directive from 2006—have to be implemented by all member states and thus have far-reaching consequences for national law. Yet so have policy revisions, such as the decision in 2014 by the Court of Justice of the European Union to revoke the Directive. Complementing these instances of "hard law," normative institutions such as the UN Special Rapporteurs on freedom of expression and on privacy influence the limits of acceptable behavior by states.

The Snowden revelations, initially, did not lead to any significant overhaul of surveillance powers in the UK. On the contrary, the revocation of the EU Data Retention Directive in 2014 led the UK government to propose and adopt the Data Retention and Investigatory Powers (DRIP) Act to continue key provisions of the Directive. Plans for a Communications Data Bill—nicknamed the "snooper's charter"—were advanced by the Conservative majority in the coalition government of 2010–2015, but halted because of resistance by the junior party in the coalition, the Liberal Democrats. One of the first announcements by Tory party

ministers on the morning of their election victory in 2015 was to move ahead with this Bill (Gayle, 2015), which would vastly expand data interception and collection.

However, several developments in the aftermath of the Snowden revelations influenced the course of the policy debate. To start with, judicial challenges of both the activities of security agencies and national legislation highlighted a need for substantial policy review. These included a successful High Court challenge to DRIPA by the MPs David Davis and Tom Watson, which declared a section of DRIPA unlawful and required new replacement legislation. Campaign organizations such as Privacy International, Liberty, and Amnesty International challenged GCHQ's surveillance practices at the Investigatory Powers Tribunal (IPT), which decided that the agency's activities were broadly compatible with the European Convention's privacy and freedom of expression guarantees, but that the sharing of data between GCHQ and NSA, and the spying on human rights organizations by GCHQ, were unlawful. Appeals of these decisions, and further lawsuits including by the civil society groups Open Rights Group, Big Brother Watch, and English PEN, were brought before the European Court of Human Rights.

Further, several institutional reviews in the first half of 2015 raised concerns with the legitimacy and legal grounding of surveillance practices. Most prominently, the Independent Reviewer of Terrorism Legislation criticized the legal framework as "obscure," "undemocratic," and "intolerable" (Anderson, 2015, p. 13) and called for a significant review and redevelopment. Further reports were published by the ISC (ISC, 2015) and the Independent Surveillance Review of RUSI (2015), which called for a "democratic license" (p. 97) for the surveillance activities of intelligence agencies.

At the international level, United Nations rapporteurs have condemned surveillance in stronger terms. A few days before the first Snowden leaks were published in June 2013, then-UN Special Rapporteur on the right to freedom of expression and opinion Frank La Rue highlighted the right to privacy as an essential requirement for the realization of the right to freedom of expression (La Rue, 2013). His successor, David Kaye, has emphasized the essential role of encryption and anonymity for people's rights to freedom of opinion and expression (Kaye, 2015), and the newly appointed Special Rapporteur on the right to privacy has criticized the surveillance practices and insufficient legal restrictions of countries such as the UK. While these UN reports have had a less immediate effect on national policy development, they have underlined and legitimized criticism from civil society and have reinforced public pressure for policy change.

British civil society organizations and campaign groups have exerted pressure by issuing statements regarding their concerns about surveillance, organizing public debates, lobbying legislators, and expanding their membership. A coalition was formed—Don't Spy On Us—which has combined some of this advocacy work toward a common campaign. Significantly, Internet companies have been increasingly vocal in their criticism of large-scale surveillance, too. Concerned about the implications of the Snowden revelations for user trust in their services, they have focused more attention on data security and user privacy, and advocated for policy reform.[4] This has introduced tensions into the relationship between governments and the corporate sector and has separated, to some extent, the powerful forces of government and Internet business (Wizner, 2015).

[4] See, e.g., https://www.reformgovernmentsurveillance.com/

These tensions have been reflected in strong pressure by British politicians and security agencies on companies to comply with data requests by the state. GCHQ Director Robert Hannigan has called social media networks "terrorists' command and control networks of choice" (Hannigan, 2014, para. 6) and then-Prime Minister David Cameron demanded that they "do more to co-operate with the intelligence agencies" (Watt & Wintour, 2015, para. 3). Both the British Prime Minister and the Home Secretary called for limits to encryption and for legal backdoors to enable data monitoring by security agencies (Temperton, 2015). Companies like Apple, on the other hand, have strongly condemned the weakening of encryption systems (Quinn, 2015).

In response to all these dynamics, the government presented comprehensive new draft legislation in October 2015 to combine the fragmented legislative framework of data collection and analysis into one law. The purpose of the Investigatory Powers Bill (IP Bill) was to regulate a wide range of surveillance practices—from bulk data collection to "computer network exploitation" (i.e., hacking). It constituted a significant shift in British surveillance policy by opening up many of the traditionally secret surveillance measures to public scrutiny and oversight. However, the substance of surveillance powers largely remained and partly expanded (as we will explore below).

The mixed picture of surveillance reform in the UK is reflected by developments elsewhere. In countries like France and Denmark, new laws to strengthen surveillance capabilities were adopted in response to recent terrorist attacks (Treguer, 2015). In the United States, on the other hand, the USA Freedom Act, which was adopted in May 2015, restricts data collection by state agencies and thus reversed a trend toward ever-increasing surveillance for the first time since the 1970s (Wizner, 2015). The communications law "Marco Civil" in Brazil provides stronger protection of citizens' privacy and anonymity online (Medeiros & Bygrave, 2015). Thus, the trend globally is differentiated, and while formal policy reform in some countries extends the legal use of surveillance capabilities, in other countries we have witnessed a pushback on state powers in light of the Snowden revelations.

Interests and Controversies: The Struggle Over Issues

The challenge of developing a commonly accepted policy framework for data collection and interception begins with the definition of "surveillance." As our interviews have shown, different stakeholders have incompatible understandings of what it means. The majority of interview participants regarded surveillance as a broad term that "refers to people being watched, monitored, data collected in almost any sense" (Interviewee 1, Pol). Surveillance, for them, starts at the point of intercepting and collecting data as this implies "the ability or the power to look into the records or the communications of individuals" (Interviewee 7, Ind). Privacy interference therefore "begins at the point of collection" (Interviewee 11, CS), which is a view supported by both surveillance studies scholars and court decisions (cf. Royal Courts of Justice, 2015, para. 114).

In contrast, members of the security sector and a minority of interviewees from politics and industry regard "surveillance as being something that is targeted against a particular agent—somebody who does something for a purpose that is tied to security" (Interviewee 4, Sec). Data collection thus "becomes

surveillance when it is actually looked at or analyzed" (Interviewee 8, Ind), that is, during "an actual targeted operation" (Interviewee 6, Sec), whereas data collection alone is merely intelligence gathering. These interviewees accepted that "privacy rights are engaged the moment the police service or an intelligence agency starts to plan a collection operation" (Interviewee 5, Sec), but maintained that "the real substantive invasion of privacy comes when the human analyst gets to see the material" (Interviewee 5, Sec).

The entry of automated profiling and machine-based analysis of datasets complicates the matter, though, as studies of big data (e.g., Kitchin, 2014) and its use in policing (e.g., Dencik, Hintz, Carey, & Pandya, 2015) have shown. Some interviewees felt that "it's probably more intrusive to have a machine . . . algorithmically assessing who is a threat and who is of interest" (Interviewee 11, CS), even though others maintained that "using automated search on specific targets is still a decision" by a human officer (Interviewee 4, Sec).

This debate has particular implications for the key element in Snowden's initial revelations and in much of the debate since—the mass or bulk collection of data. Law enforcement claims it is necessary to collect a vast trove of data to conduct (authorized and targeted) investigations of crime and threats to national security. "After an incident, when you know the identity of the suicide bomber, you need to find out who was that phone in contact with over the last couple of months, and so you need to retain that data" (Interviewee 5, Sec). Even though, personally, officers may feel "uneasy" with bulk collection, "there is no other way of doing it" (Interviewee 6, Sec). Yet civil society respondents pointed to those programs revealed by Snowden (e.g., "Karma Police") that focused not necessarily on crime or terrorism, but on collecting data on a broad range of targets that have, in the past, included human rights organizations (Interviewee 11, CS). With bulk collection being a serious intrusion into people's privacy, some declared to be "absolutely opposed to any bulk powers" (Interviewee 11, CS) and "any preemptive collection and retention just in case someone commits a crime" (Interviewee 9, Ind). Bulk powers, as several interviewees claim, are hard to justify regarding their proportionality, and the evidence of their necessity is unclear: "Lots of cases involve it, but that's not the same as it is essential. Lots of cases involve using a pencil. If there weren't any pencils, you'd use pens; the case would probably still go ahead" (Interviewee 1, Pol). Further, and in light of recent attacks in Europe that took place despite the wide availability of data, questions are raised regarding the effectiveness of mass data collection (Interviewee 2, Pol), and concerns exist about the extension of bulk powers in the IP Bill, for example, with the introduction of "thematic" (rather than individual) warrants and the collection of "Internet connection records" (i.e., people's browsing history).

With the conflict between the FBI and Apple over the accessibility of data stored on phones, the issue of encryption came to the forefront of surveillance-related controversies during the time of research. Surprisingly, then, it was the issue of least disagreement among interview participants. All highlighted the importance of strong encryption for digital business and online communication, and many recognized the risks of interfering with it. The Prime Minister's statements about preventing encryption were widely rejected (comments ranged from "naïve" to "foolish" to "wasn't briefed properly"). Yet a law enforcement official did point to the challenge that encrypted communication provides for their work (Interviewee 6, Sec). The common agenda was therefore not so much a concern for anonymity as for the preservation of user trust in the technology. The assumption of backdoors and compromised security would likely have the

"unintended consequence" of criminal networks and other target communities developing new encryption systems or going offline (Interviewee 8, Ind).

Industry representatives emphasized the need for future legislation to allow end-to-end encryption without government intervention and without liability to provide decrypted data upon government request. They accepted the need to provide customer data in response to a legal and proportionate warrant if the company is in possession of a decryption key, but not to design or rearchitect systems to allow agency access (Interviewee 7, Ind). While civil society members agreed with this approach, law enforcement noted that requiring the production of a decryption key would not be feasible if a service provider is located outside the UK or a country with which an agreement to that effect exists (Interviewee 6, Sec).

As encryption makes basic interception of communication more complex, state-sponsored hacking into a system—also called "equipment interference" or "computer network exploitation" (CNE)—will be an increasingly prominent method of surveillance. None of the interviewed stakeholders rejected the possibility of targeted hacking of a particular device to find information about a particular person, provided it was "controlled and limited" (Interviewee 7, Ind), "appropriately authorized, well documented, and well overseen" (Interviewee 10, CS), but bulk hacking (as allowed by the IP Bill) was widely seen as highly problematic. As inserting malware on a particular software can affect thousands of users and can potentially spread, the proportionality of such measures is particularly difficult to assess. Bulk hacking was thus described as "absurd and dangerous" (Interviewee 11, CS). Further, with the emerging Internet of Things, connected and thus exploitable devices encompass household items, cars, medical equipment, and public utilities, and the consequences of hacking such devices are difficult to foresee. For law enforcement, this brings about a vast new set of data sources ("We're getting quite excited about the Internet of Things," Interviewee 6, Sec) but also a particular need for safeguards and oversight.

Controversies over oversight have focused on both its scope and the actors involved. Interviewees from the law enforcement and intelligence sector pointed to the need for political accountability (Interviewee 4, Sec) and thus political review (Interviewee 5, Sec). Most others highlighted the need for independent judicial oversight and technological expertise (e.g., Interviewees 7 & 8, Ind). The inclusion of technical skills and broader (including civil society) perspectives in oversight regimes would be necessary, as was noted, for complex decisions in emerging areas such as CNE and automated data filtering (Interviewee 13, Rev). With GCHQ intercepting 50 billion communications a day and the Home Secretary signing several thousand warrants a year, judges would need to be equipped with adequate time and capacity to review requests, and those requests would require a high level of specificity to properly consider proportionality (Interviewee 10, CS).[5]

Finally, Internet traffic inevitably involves cross-border flows, which provides challenges for national regulation. First, the extraterritorial reach of legislation such as the IP Bill may contradict laws in other countries, and companies overseas may thus be forced to comply with different and potentially

[5] The new Investigatory Powers Commission will include a bench of judges, but falls short of these broader proposals.

incompatible laws (Interviewee 7, Ind). Second, UK law may serve as a model for other countries to address digital surveillance, which may exacerbate the problem of extraterritoriality and make UK companies subject to legislation elsewhere. To address this issue and avoid "an absurd patchwork of laws" (Interviewee 9, Ind), several interviewees pointed to the need for international agreements, particularly an international framework for data sharing. Third, the international dimension of comprehensive UK legislation highlights its normative and symbolic character. Civil society members were particularly worried that "Britain will be a global leader in surveillance. . . . Is this something that we want to export? Is this the kind of standard setting that we want to be making for the world?" (Interviewee 10, CS).

The Role of Social Forces: Impacts on Policy Change

The role of the Snowden revelations in triggering policy reform was widely accepted among interviewees. By exposing the secret practices of intelligence agencies, Snowden enabled a both public and political debate. This vindicated those (typically from civil society) who had previously warned against surveillance, and it alerted Parliamentarians "that a lot of what we had been told was rather incomplete" (Interviewee 1, Pol). It led to the reviews mentioned (Anderson, 2015; ISC, 2015; RUSI, 2015), which "pushed the idea that powers should be more explicit" (Interviewee 1, Pol). The post-Snowden climate, as one campaigner noted, forced committees such as the ISC "to look strong, as a genuine and legitimate body" (Interviewee 10, CS) and opened an opportunity for in-depth and critical investigations. The legal challenges against surveillance which provided further urgency for policy reform relied on the Snowden documents, too: "We have the Snowden documents as a compass . . . you need a compass to know what you're aiming at" (Interviewee 10, CS). Most interviewees agreed that the policy reform debate "would not have happened without Snowden."

Snowden also had significant effects on the business sector and triggered its involvement in policy reform. The leaks "made industry furious" (Interviewee 9, Ind) as they exposed, for example, practices of hacking into corporate servers. They led to a "massive loss in confidence from users [which] had large ramifications for industry [and] resulted in a lot of work to try and regain that trust" (Interviewee 7, Ind). Customers have become particularly "wary of the relationship between the security services and companies" (Interviewee 7, Ind). Further, mistrust in U.S.- and UK-based cloud services has led to "inefficiencies by continuing to invest in noncloud ways of doing things" (Interviewee 8, Ind) and has risked competitive disadvantages for British businesses as "those same concerns we're already seeing with Western European businesses not wanting to deal with an American company could start happening to UK based companies as well" (Interviewee 8, Ind).

The effect of the Snowden revelations was also acknowledged by security and intelligence experts who noted that "Snowden has pushed the policy debate forward and forced us to review policy" (Interviewee 4, Sec). The leaks required security agencies "to talk about these issues more and more, and rightly so," in the words of one officer, as "we police by consent in this country and we're dependent on people tacitly supporting our activities" (Interviewee 6, Ind). Yet these would be agreeable side effects of revelations that were otherwise deemed illegitimate as, according to this section of interviews, Snowden exposed intelligence capabilities to criminals, led to the shutdown of necessary information feeds, and thereby "pulled the rug out from under us" (Interviewee 6, Ind). One intelligence expert questioned Snowden's role for policy reform

more substantially and pointed instead to a historic process of bringing the state's secret activities under the rule of law, and interpreted the [at the time of the interview] draft IP Bill as the end of this process. "Would this have happened without Snowden? I think it would, but it [the leaks] accelerated the recognition that this final stage of the rule of law should be put in place" (Interviewee 5, Ind).

If Snowden triggered, or at least accelerated policy change, development and implementation of reform would depend, first of all, on government, Parliament, and the political context. Until 2015, the Liberal Democrat Party—as junior partner in the coalition government—offered some resistance to the expansion of surveillance powers and represented a voice for critical perspectives from civil liberty groups and the technology industry. Generally, however, the response to Snowden "was astonishingly muted" (Interviewee 1, Pol) in Parliament. Partly this was due to a lack of understanding of complex technical issues, and of "the time and exposure to be able to get the knowledge that this world sometimes demands" (Interviewee 3, Pol). In both the Commons and the Lords, members have had to deal with a variety of issues:

> We've got all this other . . . legislation coming through—the Housing Bill, the Energy Bill. From a human rights point of view, they're probably more widespread than the surveillance issue and so a lot of Peers are directing their energies to those. (Interviewee 2, Pol)

Furthermore, criticism of security agencies is rare. As a former MP noted, "I think there's a certain deference to agencies here, unlike the U.S. which has experience of McCarthy and all sorts of other intelligence gone wrong scenarios, and unlike Germany" (Interviewee 1, Pol). In addition, some MPs were subjected to pressure from government "to defend the agencies" (Interviewee 1, Pol). Both the Commons and the Lords eventually adopted the Bill despite a lack of substantial revisions that had been demanded by a wide range of experts and stakeholders (see below) as well as parliamentary review committees.[6] Parliamentary control of government was thus ineffective.

This role was occupied in part by civil society. Whereas historically, campaign groups and advocacy organizations were not involved by government in internal surveillance policy debates, they have increasingly been recognized as a legitimate actor with relevant expertise and are "less being seen as the angry voice and rather as a useful collaborative voice" (Interviewee 12, CS). This, however, has affected civil society strategies as the classic approach of opposition to surveillance has, in some cases, given way to a more nuanced discussion: "Previously NGOs would have fought just to kill a new law and probably been unsuccessful in doing so; now they can say: here's how we can genuinely improve it and have a proper conversation with the Home Office" (Interviewee 10, CS). This has enabled civil society to participate in a key policy process, but it has also risked the normalization of surveillance as principled opposition is replaced by collaboration, and it has exposed differences in civil society agendas. While some value "the ability now to have very complicated policy discussions with intelligence officials" (Interviewee 10, CS) and aim at "chipping away at the mountain of surveillance rather than trying to take the whole thing down" (Interviewee

[6] See http://www.parliament.uk/business/committees/committees-a-z/joint-select/draft-investigatory-powers-bill/news-parliament-2015/report-published/

12, CS), others fear that a focus on the specifics of the IP Bill—and the new friendliness with security agencies—have compromised civil society principles regarding a more fundamental review of surveillance practices. "Some are still steadfast, but I think some are now thinking: How can we just get things to be better? Some, not all, are slightly more accepting of the basic premise of bulk data collection" (Interviewee 11, CS). The diverse positions of civil society organizations were reflected in the large amount of submissions to review processes and many public statements, but hardly affected the various drafts of the policy text.

The technology business sector served as the other voice of strong criticism against an expansion of surveillance capabilities (see aforementioned), and large Internet companies like Apple, Facebook, and Google issued common statements in condemnation of key parts of the IP Bill,[7] but just like the civil society contributions, these received little traction. Access by industry to the policy development process was better than that of civil society, and business was consulted in the early stages of drafting (Interviewee 7, Ind). Despite that, industry representatives did not feel that their opinions were taken on board.

Security and intelligence agencies were involved in policy reform discussions from the outset and were thus able to shape the new legislation in more detail. For example, the time frame of one year for data retention, as adopted in the IP Bill, was based on a suggestion by the National Crime Agency (Interviewee 5, Sec) and it was not changed despite heavy criticism from most other participants and observers. Even though agency officials claim that not all their concerns were incorporated in the bill (Interviewee 6, Sec), they enjoyed the closest access to decision makers. They benefited from an institutional arrangement that placed the Home Office (which is responsible for domestic security) at the center of the policy reform process, which provided security and intelligence agencies with a "hotline" (Interviewee 1, Pol) to lawmakers, while interests that may have offered a counterbalance (civil liberty, freedom of expression, and privacy) were based at the Ministry of Justice and thus outside the core process. Further, agency concerns received support from the Home Office's Director General of Security and Counterterrorism who, according to a former Parliamentarian, "saw his role not as a filter, but as an advocate" (Interviewee 1, Pol) for the expansion of surveillance powers.

Different levels of access to decision makers thus played a significant role in the shaping of policy reform. While most of the publicly available consultations were critical of the proposed Bill, the supporters of the Bill had internal communication channels at their disposal and managed to advance their interests through those without major resistance. The agendas of law enforcement and agencies to expand data collection and demand more powers follow logically from their social role and remit, yet the institutional processes of balancing benefits and risks by incorporating different perspectives were underdeveloped.

A Democratic License? Transparency and Public Debate

A key criticism of the reviews published in 2015 was the obscure nature of the policy framework in the UK. Accordingly, the increase in transparency of the new Bill was widely acknowledged. Business representatives supported "the effort of bringing together all these different pieces of counterterrorism and surveillance legislation under one single Bill" (Interviewee 7, Ind) "within a well-understood, controlled, and regulated framework" (Interviewee 8, Ind). Civil society members applauded "the fact that it is the most

[7] http://www.publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/Memo/IPB21.htm

transparent bit of legislation that Britain's ever had" (Interviewee 10, CS), and law enforcement officials praised the "clearer framework and clearer guidelines" for their work (Interviewee 6, Sec) that codify "how under the rule of law you can encompass activity which is, the public thinks, necessary" (Interviewee 5, Sec).

Beyond the general recognition of improved transparency, however, views differ widely on whether the Bill can provide the "democratic license" that the RUSI report (2015) called for. The core of the critique has been that an opportunity for a fundamental review of surveillance practices and capabilities was lost. Instead, the main purpose of the new law was seen "to justify essentially previous secret practice" (Interviewee 10, CS): It is aiming "to legitimize existing behavior rather than to enter into a debate about what should be done" (Interviewee 10, CS). In the words of a Peer in the House of Lords: "This Bill is covering their backs. It's saying that all these things they've been doing for years will now be legal. It's a bit like pulling a skirt down after you've exposed your ankles" (Interviewee 2, Pol).

The Snowden revelations called for a broader public debate on surveillance practices and the development of the Bill could have been an occasion to have this societal conversation. However, most interviewees agreed that a true public debate has not yet taken place. While debates on, for example, bulk collection were happening in the United States and elsewhere, "we haven't had the chance to have that in the UK" (Interviewee 7, Ind). On the contrary, just as earlier legislation (DRIPA) had been rushed through Parliament under the pretense of an "emergency" (Interviewee 11, CS), it was criticized that the timetable for Parliamentary review of the Bill did not leave sufficient time for expert scrutiny, let alone public debate. Members of the law enforcement community recognized that "we should have a public debate" (Interviewee 6, Sec), but maintained that a certain level of secret intelligence would be necessary and inevitable. Therefore the public would need to trust in the new processes, including its oversight mechanisms, as "the best device that democracy has come up with is trust by proxy" (Interviewee 5, Sec). However this view is unlikely to convince those who maintain that the abuse of trust by state agencies lies at the core of the surveillance problem.

The limited debate that did take place, some felt, was dominated by a security discourse and—similar to the policy development—by information provided through intelligence agencies, government and law enforcement. These actors "are in control of the information that we have and that we don't have and therefore are able to move the goalposts of the debate" (Interviewee 11, CS). Overall, while transparency and openness have been a key factor in the recent UK policy debate, most stakeholders—for varying reasons—would agree that an extensive public discussion on the future of surveillance policy has not yet taken place.

Digital Citizenship and the State

If citizenship denotes people's role in democratic society, their active engagement with their environment, and their relation with the state, surveillance policy affects all these aspects. It regulates the digitally mediated ways in which individuals increasingly interact with society (and which include some of the most intimate parts of people's lives); it constrains the extent of privacy and free communication that is available; and it redefines the power of the state vis-à-vis its citizens. Yet the standards by which

surveillance policy is discussed and decided, in these current times, are questions of security—more specifically, "a very unique and defined area of national security" (Interviewee 4, Sec) rather than other possible concerns around, for example, human security. This focus on national security highlights the needs of the state, and it serves as a dominant framework of debate. It emphasizes the role of security services, and it deprioritizes other concerns (Interviewee 2, Pol).

Several interviewees emphasized the need to, instead, start the discussion from the citizen's perspective and "flip the switch from state- to citizen-centric thinking" (Interviewee 3, Pol). The focus, according to a business representative, should not be to make the life of intelligence agencies and law enforcement easier, but on the stability and safety of technical infrastructure and the security of the user (Interviewee 8, Ind). An intelligence expert expressed the hope that the combination of the Snowden revelations with the recognition of persistent terror threats would lead to "digital reconciliation in which these different currents of opinion come together—privacy concerns, concerns about oversight, and concerns about security and public safety" (Interviewee 5, Sec).

Despite the acceptance that security risks exist, other participants maintained that bulk data collection, in particular, leads to a transformation in the nature of the relationship between the citizen and the state. It means that all citizens' most personal data and communication is potentially scrutinized, searched, and profiled, and that citizens become suspects, particularly if they choose to exert their privacy and apply measures against the collection of their data (Interviewee 11, CS). The particular significance of this shift in power between state and citizen through surveillance policy lies in the risk of surveillance for constraining free expression, dissident communication and organizing, and other key elements of digital citizenship. An overreach in surveillance capabilities and practices may thus lead to sustained degradation of democracy (Interviewee 11, CS).

This research has focused on state-based data collection and surveillance as the latter is highlighted by both the Snowden revelations and the recent UK policy reform. As noted, vast amounts of personal data are also collected and analyzed by Internet businesses, and several interviewees (particularly from the security community) pointed to the risks associated with these practices. Others defended the focus on state surveillance as, they said, it takes place in secret, without consent, and may have legal and safety-related repercussions (Interviewee 9, Ind). A concern with digital citizenship must not forget the implications of private sector-based data collection, but will necessarily emphasize the dimension of state–citizen relations.

Conclusion

The Snowden revelations have opened a policy window for debates on legislative reform. A combination of legal challenges, parliamentary reviews, and normative interventions forced the UK government to develop a new legislative framework whose openness and transparency has been praised. However, as we have seen, intense controversies over both the broader direction and the details of surveillance policy, as well as the very definition of surveillance, prevail. While the development of a new law has facilitated an exchange between different stakeholders and led to a more nuanced relationship between them, fundamental differences in opinion remain regarding both the substance of and the process toward the new legal framework.

Different levels of access to decision makers as well as specific institutional settings have led to unequal degrees of influence over policy reform and an imbalance in the voices and interests that are represented. Even though the vast majority of public contributions and review commissions (as well as interview participants for this study) were critical of the proposed legal frameworks of data collection, the interests of the intelligence and law enforcement sector succeeded in framing the debate. The current national security discourse that prioritizes the state's role in protecting against physical harms over citizens' privacy and civil rights has provided the context for this imbalance. As a result, the Investigatory Powers Bill has codified, maintained, or even expanded current surveillance capabilities. Policy reform in the UK has not led to a fundamental revision of surveillance practices, nor to a broader public debate that would help to democratically legitimize these practices.

The fact that some (limited) policy review and debate took place and led to a more transparent legislative framework with a public avowal of all (known) surveillance capabilities may enhance the informed exercise of digital citizenship. However the range of data collection capabilities—from interception to network exploitation—constrains the possibilities of unimpeded digital expression and engagement. The new legal framework therefore causes a power shift, according to most of our interviewees, from citizens to the state. Yet our research also shows that the environment for digital citizenship is very much in flux and is affected by a complex interplay of forces, interests, and public discourses. Changes in national political coalitions, institutional settings, international pressures, business interests, advocacy strategies, security incidents, and public perception can shift the understandings of what is feasible and desirable. The shaping of a regulatory framework for digital citizenship is therefore ongoing.

References

Anderson, D. Q. C. (2015). *A question of trust—report of the Investigatory Powers Review (June 2015)*. Retrieved from https://terrorismlegislationreviewer.independent.gov.uk/a-question-of-trust-report-of-the-investigatory-powers-review/

Andrejevic, M. (2012). Exploitation in the data mine. In C. Fuchs, K. Boersma, A. Albrechtslund, & M. Sandoval (Eds.), *Internet and surveillance: The challenges of Web 2.0 and social media* (pp. 71–88). Abingdon, UK: Routledge.

Bakir, V. (2015). The veillant panoptic assemblage: Mutual watching and resistance to mass surveillance after Snowden. *Media and Communication, 3*(3), 12–25.

Brown, I. (2014). *National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies: United Kingdom* (Report for European Union Agency for Fundamental Rights). Retrieved from fra.europa.eu/sites/default/files/fra_uploads/united-kingdom-study-data-surveillance-uk.pdf

Chakravartty, P., & Zhao, Y. (2008). *Global communications: Towards a transcultural political economy*. Lanham, MD: Rowman & Littlefield.

Council of Europe. (1950). *European Convention of Human Rights*. Retrieved from https://www.echr.coe.int/Documents/Convention_ENG.pdf

DeNardis, L. (2009). *Protocol politics: The globalization of Internet governance*. Cambridge, MA: MIT Press.

Dencik, L., Hintz, A., Carey, Z., & Pandya, H. (2015). *Managing "threats": Uses of social media for policing domestic extremism and disorder in the UK* (Project report, Cardiff University). Retrieved from http://www.dcssproject.net/files/2015/12/Managing-Threats-Project-Report.pdf

European Parliament. (2001, July 11). *Report on the existence of a global system for the interception of private and commercial communications* (ECHELON interception system) (2001/2098(INI)). Retrieved from http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A5-2001-0264+0+DOC+XML+V0//EN

Fidler, D. P. (Ed.). (2015). *The Snowden reader*. Bloomington: Indiana University Press.

Freedman, D. (2008). *The politics of media policy*. London, UK: Polity Press.

Gayle, G. (2015, May 9). Theresa May to revive her "snooper's charter" now Lib Dem brakes are off. *The Guardian*. Retrieved from http://www.theguardian.com/politics/2015/may/09/theresa-may-revive-snoopers-charter-lib-dem-brakes-off-privacy-election

Gürses, S., Troncoso, C. G., & Diaz, C. (2011). *Engineering privacy by design*. Paper presented at Computers, Privacy & Data Protection, Brussels, Belgium. Retrieved from https://www.cosic.esat.kuleuven.be/publications/article-1542.pdf

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *British Journal of Sociology*, *51*(4), 605–622.

Hampton, K. N., Rainie, L., Lu, W., Dwyer, M., Shin, I., & Purcell, K. (2014). *Social media and the "spiral of silence."* Washington, DC: Pew Research Center. Retrieved from http://www.pewinternet.org/files/2014/08/PI_Social-networks-and-debate_082614.pdf

Hannigan, R. (2014, November 3). The Web is a terrorist's command-and-control network of choice. *Financial Times*. Retrieved from http://www.ft.com/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdc0.html#axzz3TywRsOQ2

Held, D., & McGrew, A. G. (2003). The great globalization debate. In D. Held & A. G. McGrew (Eds.), *The global transformations reader* (pp. 1–50). Cambridge, UK: Polity Press.

Hintz, A. (2015). Social media censorship, privatised regulation, and new restrictions to protest and dissent. In L. Dencik & O. Leistert (Eds.), *Critical perspectives on social media and protest: Between control and emancipation* (pp. 35–52). Lanham, MD: Rowman & Littlefield.

ISC (Intelligence and Security Committee of Parliament). (2015) *Privacy and security: a modern and transparent legal framework.* Retrieved from http://isc.independent.gov.uk/files/20150312_ISC_P+S+Rpt(web).pdf

Isin, E., & Ruppert, E. (2015). *Becoming digital citizens*. Lanham, MD: Rowman & Littlefield.

Kaye, D. (2015). *Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression*. Retrieved from http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/OpinionIndex.aspx

Keck, M. E., & Sikkink, K. (1998). *Activists beyond borders: Advocacy networks in international politics*. Ithaca, NY: Cornell University Press.

Kingdon, J. W. (1984). *Agendas, alternatives, and public policy*. Boston, MA: Little, Brown.

Kitchin, R. (2014). *The data revolution: Big data, open data, data infrastructures & their consequences*. London, UK: SAGE Publications.

La Rue, F. (2013, April 17). *Report of the special rapporteur on the promotion and protection of the right to freedom of expression*. Retrieved from http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

Lessig, L. (1999). *Code and other laws of cyberspace*. New York, NY: Basic Books.

Lyon, D. (2014, July–December). Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society,* 1–13.

Medeiros, F. A., & Bygrave, L. A. (2015). Brazil's Marco Civil da Internet: Does it live up to the hype? *Computer Law and Security Review, 31*(1), 120–130.

Meyer, D. S. (2005). Social movements and public policy: Eggs, chicken, and theory. In D. S. Meyer, V. Jenness, & H. Ingram (Eds.), *Routing the opposition: Social movements, public policy, and democracy* (pp. 1–26). Minneapolis: University of Minnesota Press.

Mueller, M. (2010). *Networks and states: The global politics of Internet governance*. Cambridge, MA: MIT Press.

Musiani, F. (2015). Practice, plurality, performativity, and plumbing: Internet governance research meets science and technology studies. *Science, Technology & Human Values, 40*(2), 272–286.

PEN. (2013). *Chilling effects: NSA surveillance drives U.S. writers to self-censor*. New York, NY: Author. Retrieved from http://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf

Quinn, B. (2015, November 10). UK surveillance bill could bring "very dire consequences," warns Apple chief. *The Guardian*. Retrieved from http://www.theguardian.com/world/2015/nov/10/surveillance-bill-dire-consequences-apple-tim-cook

Raboy, M. (2002). *Global media policy in the new millennium*. Luton, UK: University of Luton Press.

Raboy, M., & Padovani, C. (2010). Mapping global media policy: Concepts, frameworks, methods. Retrieved from http://www.globalmediapolicy.net/sites/default/files/Raboy&Padovani%202010_long%20version_final.pdf

Royal Courts of Justice. (2015). Davis & Others v The Secretary of State for the Home Department. Citation Number: [2015] EWHC 2092 (Admin). Case No: CO/3665/2014, CO/3667/2014, CO/3794/2014. 17 July 2015. Retrieved from https://www.judiciary.gov.uk/wp-content/uploads/2015/07/davis_judgment.pdf

RUSI (Royal United Services Institute). (2015). *A democratic licence to operate: Report of the Independent Surveillance Review*. Retrieved from https://rusi.org/publication/whitehall-reports/democratic-licence-operate-report-independent-surveillance-review

Temperton, J. (2015, July 15). No u-turn: David Cameron still wants to break encryption. *Wired*. Retrieved from http://www.wired.co.uk/article/cameron-ban-encryption-u-turn

Treguer, F. (2015, April 29). France's Intelligence Bill: Legalizing mass surveillance. *Open Democracy*. Retrieved from https://www.opendemocracy.net/digitaliberties/f%C3%A9lix-tr%C3%A9guer/france%E2%80%99s-intelligence-bill-legalises-mass-surveillance

Trottier, D. (2015). Open source intelligence, social media and law enforcement: Visions, constraints and critiques. *European Journal of Cultural Studies, 18*(4–5), 530–547.

Watt, N., & Wintour, P. (2015, January 16). Facebook and Twitter have social responsibility to help fight terrorism, says Cameron. *The Guardian*. Retrieved from http://www.theguardian.com/world/2015/jan/16/cameron-interrupt-terrorists-cybersecurity-cyberattack-threat

Wizner, B. (2015, June 18). *Keynote address to the conference "Surveillance and Citizenship."* Cardiff, UK: Cardiff University.

Youmans, W. L., & York, J. C. (2012). Social media and the activist toolkit: User agreements, corporate interests, and the information infrastructure of modern social movements. *Journal of Communication*, *62*, 315–329.